

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with Apple ID
barasnehyousef@gmail.com that is stored
at premises controlled by Apple

Case No. 20-878M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B


The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 241

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Jessica Krueger

Printed Name and Title

Sworn to before me and signed in my presence:

Date: January 24, 2020



Judge's signature

City and State: Milwaukee, Wisconsin

Case 2:20-mj-00878-NJ Filed 02/13/20 Page 1 of 31 Document 1

Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jessica Krueger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with an Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the FBI and have been since November 2009. I am involved in investigations of persons suspected of violations of Federal law in the State of Wisconsin and throughout the United States. I have gained experience conducting investigations through formal training and consultation with local, state, and federal law enforcement agencies as well as from law enforcement investigations themselves. I have assisted in multiple criminal investigations and participated in numerous search and arrest warrants related to such investigations

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. § 241, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating criminal activity by members of an organization called “The Base,” a neo-Nazi group that aims to unify militant white supremacists around the globe and provide them with paramilitary training in preparation for a “race war.” As described herein, Yousef Omar Barasneh is a member of “The Base,” and in September 2019, he conspired with others and participated in vandalizing a synagogue in Racine, Wisconsin, in violation of, among other things, and 18 U.S.C. § 241, which makes it a felony to “conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free exercise or enjoyment of any right or privilege

secured to him by the Constitution or laws of the United States.” Relatedly, 42 U.S.C. § 1982, secures the right of all U.S. citizens to hold and use real and personal property, including property used for religious purposes.

7. On January 17, 2020, Barasneh was arrested on a criminal complaint issued in this district charging that in September 2019, Barasneh violated 18 U.S.C. § 241. See Case No. 20-MJ-861. He made his initial appearance that day before U.S. Magistrate Judge William E. Callahan. Barasneh was thereafter released from custody subject to conditions set by the Court. Below is background information regarding the investigation relevant to the requested warrant.

8. On September 22, 2019, law enforcement officers in Wisconsin discovered that the Beth Israeli Sinai Congregation located at 3009 Washington Avenue Racine, Wisconsin, had been vandalized. Specifically, the officers saw swastikas, the symbol for The Base, and anti-Semitic words spray-painted on the exterior of the building. The synagogue is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

9. Similarly, on September 21, 2019, law enforcement officers in Hancock, Michigan, discovered that the Temple Jacob had been vandalized. Specifically, they saw swastikas and the symbol of The Base spray-painted on the exterior of the building. As with the synagogue in Racine, Wisconsin, the synagogue in Michigan is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

10. Based on my training and experience and familiarity with this investigation, I am aware that The Base is a white, racially-motivated extremist group that describes itself as an “international survivalism & self-defense network, for nationalists of European descent,” and offers “IRL” (in real life) survivalist training to resist “our People's extinction,” or the extinction of the white race. Members of The Base communicate with each other through online platforms and encrypted online messaging applications and chat rooms. In these communications, they have discussed, among other things, acts of violence against minorities (including African Americans and Jewish-Americans), Base military training camps, and ways to make improvised explosive devices (“IEDs”). The symbol used by The Base is a black flag with three white Runic Eihwaz symbols.

11. Based on information I have received during the course of this investigation, I am aware that The Base has been active in Wisconsin and that there are members of the “North Central region,” alternatively known as the “Great Lakes cell,” based in Wisconsin. For instance, in early June 2019, Base recruitment flyers were posted at Marquette University in Milwaukee, WI. In July 2019, The Base organized an armed training session for members in Wood County, Wisconsin, and posted photos to social media about the session. And, as noted above, the symbol for The Base was discovered spray-painted on the Beth Israel Sinai Congregation synagogue in Racine, WI.

12. As part of the investigation, the FBI received information from an individual associated with The Base, who I will refer to as co-conspirator #1 ("CC1"). In statements to the FBI between October 2019 and December 2019, CC1 admitted that in September 2019, he directed other members of The Base to vandalize minority-owned properties throughout the country. CC1 called this "Operation Kristallnacht"¹ and directed others to "tag the shit" out of synagogues. Based on my training and experience and familiarity with this investigation, I believe that CC1 meant that synagogues should be spray-painted with anti-Semitic graffiti. CC1 further elaborated on his instructions to other Base members, stating that "if there's a window that wants to be broken, don't be shy." CC1 told the FBI that the operation was nationwide, and that CC1 knew members of The Base's Great Lakes cell carried out attacks against synagogues in Wisconsin and Michigan.

13. CC1 stated that the person who carried out the attack on the synagogue in Racine, Wisconsin, was a Base member known as "Joseph" or "Josef." CC1 stated that Joseph was a member of The Base's Great Lakes cell and was from Wisconsin. CC1 stated that Joseph joined The Base around March 2019, and had been vetted by the group's leader. According to CC1, after the Racine synagogue

¹ Based on publicly available information, I am aware that Operation Kristallnacht, or the Night of Broken Glass, is an event that occurred in Nazi Germany on November 9 and 10, 1938. During this time, Jewish homes, hospitals, and schools throughout Germany were ransacked and demolished by Nazi paramilitary soldiers and civilians. The name "Kristallnacht" comes from the shards of broken glass that littered the streets after the windows of Jewish-owned stores, buildings, and synagogues were smashed.

attack, Joseph sent CC1 a message on an encrypted platform with a news article about the attack and wrote something to the effect of "here's what I did."

14. CC1 stated that CC1 had never met Joseph in person. But, they had communicated with each other via an encrypted message application, which can be accessed via computer, cell phone, or other electronic device such as a tablet. This includes being accessible through an application installed on a device such as a cell phone. CC1 knew Joseph to be a large individual. CC1 and Joseph had planned to meet in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting.

15. Information provided by CC1 has been corroborated by investigators. For instance, in November 2019, the FBI obtained a search warrant for CC1's residence and electronic devices. In CC1's electronic devices, investigators found evidence showing that that around September 17, 2019, and again on September 21, 2019, CC1 conducted multiple Google searches for "Kristallnacht." Following the search for "Kristallnacht" on September 17, 2019, CC1 used an internet browser to access an encrypted messaging application known to be utilized by members of The Base. The digital evidence showed that CC1 accessed the encrypted messaging application and visited a section of the application that was labeled with the symbol for The Base.

16. On September 23, 2019, CC1 conducted multiple Google searches for "racine, wi," "racine wi nazi," and "racine wi anti-semitic." CC1 also accessed news

websites and Twitter that had posted articles and comments on the Racine synagogue vandalism. Further, the device evidence shows that on September 23, 2019, CC1 accessed the same encrypted messaging application noted above. The evidence showed that CC1 accessed a section of the encrypted messaging application that was labeled with "JOSEPH." Based on my training and experience and my involvement in this investigation, I believe that CC1 was using the encrypted messaging application to exchange messages with members of The Base, including "JOSEPH."

17. As part of the FBI's investigation into the Base, an FBI undercover employee (UCE) gained access The Base's members-only chat room on the encrypted messaging application discussed above. This included a group chat in September 2019 among several individuals in which CC1, utilizing his known Base online moniker, urged other members of the group chat to respond to the doxing² of a Base member. CC1 directed that between September 20-25, 2019, CC1 wanted them to "get out and act. Flyers, windows, and tires." He also told members of the group chat that arsons, breaking windows, and slashing tires are near impossible to track. In response to CC1's call to action, a chat member named "Joseph" responded "I

² Based on publicly available information, I am aware that "doxing" is the online practice of researching and broadcasting private or identifying information about an individual or organization. The methods employed to acquire this information include searching publicly available databases and social media websites, hacking, and social engineering. Doxing is often done with malicious intent.

agree with that . . . calculated action” and tagged CC1’s online moniker. Joseph went on to write “imagine if across the country on local news, Everyone is reporting on new nazi presence.” CC1 in the same chat wrote “20th—25th, vandalize my friends. We’ll push back on the enemy as they push bacjk [sic].” Another member of the chat wrote “No point in random vandalizing... Much more effective if its targeted,” to which Joseph responded “^^ MAKE IT WORTH IT.” As part of the chat, CC1 wrote “Kristallnacht” and Joseph wrote “Take your time, plan your out your AO.” Later on in the group chat, Joseph wrote “Our op will be a perfect fuck you to these kikes if we become terrorists.” CC1 later wrote a long entry titled “Operation Kristallnacht,” discussing why this was the time to act, to which Joseph responded “Sieg Heil.”

18. CC1 has been arrested and charged in another federal district court with violating 18 U.S.C. § 241. The charges relate to CC1’s conduct in directing other Base members to attack synagogues in Racine, Wisconsin, and Hancock, Michigan, as described above.

19. As noted above, during CC1’s interviews with the agents, he stated that he had planned to meet Joseph in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting. As discussed below, that Base meeting did occur in Silver Creek, Georgia, from about October 30, 2019 until November 2, 2019, and that the Base member known as Joseph attended the meeting.

20. Between October 31 and November 3, 2019, the UCE participated in an “in real life” or “IRL” meeting of The Base at the residence of a Base member in Silver Creek, Georgia. About a dozen individuals participated in the event, including the Base member known as Joseph. The meeting included firearms training, grappling, basic medical training, and a pagan “blot” ritual where a goat was sacrificed. UCE observed Joseph participate in many of these activities.

21. The Base member known as Joseph was observed by the FBI arriving and departing this meeting while driving a dark GMC SUV bearing Wisconsin license plate 671NGF. Records show that the vehicle is registered to Barasneh’s known residence in Oak Creek, Wisconsin.

22. I have reviewed images of “Joseph” from the Base meeting in Georgia, and Barasneh’s Wisconsin Driver’s License photo, and I believe that The Base member known as Joseph is Barasneh. Further, on November 15, 2019, November 25, 2019, December 5, 2019, and January 10, 2020, FBI agents observed Barasneh driving the GMC SUV bearing Wisconsin license plate 671NGF in and around Oak Creek, Wisconsin.

23. As part of the investigation, I reviewed information from Wyndham Hotels and Resorts showing that on October 30 to 31, 2019, Barasneh registered to stay at a La Quinta Inn located in Rome, Georgia, and provided his known home address in Oak Creek. That hotel is approximately seven miles from the Base

residence in Silver Creek, Georgia, where the Base meeting took place that same weekend.

24. As part of the investigation, FBI agents identified several dates and locations where members of the Base were believed to have been. This included (1) July 27, 2019, the date that The Base conducted training at the Wood County Firing Range, Town of Seneca, Wood County, WI; and (2) the evening of September 21, 2019, when the Beth Israeli Sinai Congregation located in Racine, Wisconsin, was vandalized. Thereafter, pursuant to a court order, agents obtained information about cell phone connections to towers near those locations on those dates. The cell tower information revealed that, on July 27, 2019, between 7:00 a.m. and 7:00 p.m., a device with telephone number 414-XXX-8150 pinged approximately 78 times off the tower close to the Wood County Firing Range, Town of Seneca, Wood County, WI. The information further showed that on September 21, 2019, between 8:38 p.m. and 9:08 p.m., the device with that number pinged approximately 6 times off the tower close to 3009 Washington Avenue, Racine, Wisconsin.

25. Records obtained from AT&T show that during the relevant time period, the phone number 414-XXX-8150 was issued to subscriber O.B. and user Yousef BARASNEH, with a billing address of BARASNEH's known residence in Oak Creek, Wisconsin. The records from AT&T state that the phone number is associated with an Apple iPhone 6S with IMEI 3557670792347715, though I understand that phone numbers may be ported among devices at any time. Police

records further show that on October 24, 2017, BARASNEH had contact with the Oak Creek Police Department and reported to the officers that 414-XXX-8150 was his phone number. Records from AT&T further show that, between October 30 and November 2, 2019, the device with phone number 414-XXX-8150 connected with cell towers near Rome, Georgia, and Silver Creek, Georgia.

26. On January 16, 2020, the U.S. District Court for the Eastern District of Wisconsin issued a criminal complaint and arrest warrant for Yousef Omar Barasneh, as well as a search warrant for Barasneh's residence in Oak Creek, Wisconsin. Early in the morning on January 17, 2020, FBI agents executed the search warrant at the residence in Oak Creek, Wisconsin. When the FBI entered the residence, Barasneh was in his bedroom with the door locked. Agents announced their presence, but it took Barasneh several seconds to open the door, during which time the FBI could hear Barasneh moving around. When he did open the door, he was placed under arrest. Next to the door on a dresser, agents found an iPhone 6s mobile device. An examination of the phone later that same day revealed that the device was unlocked at approximately the same time the FBI was attempting to arrest Barasneh. This indicated that Barasneh likely opened and accessed his phone before opening the door. Based on the investigation, it is reasonable to infer that Barasneh may have been attempting to delete items relevant to the investigation from the device knowing that the FBI would immediately seize it.

27. A subsequent examination of that phone by the FBI revealed that the device was named "Yousefs iphone," it was associated with Apple ID barasnehyousef@gmail.com, and that the number assigned to the phone was 414-XXX-8150. The examination also showed that iCloud was active on the phone with a backup to the iCloud happening as recently as November 20, 2019.

28. According to information received from Apple on January 6, 2020, an Apple account with ID barasnehyousef@gmail.com is subscribed to Yousef Barasneh, telephone number 414-XXX-8150, and address of Yousef's residence in Oak Creek, Wisconsin. The Apple account includes an active iCloud and on May 15, 2019, an iPhone 6s was linked to the iCloud.

29. From my training and experience, I know that the iCloud is a cloud storage and cloud computing service that Apple provides to its customers and is accessible on their products, including the iPhone. Customers can use the iCloud to backup information, to include SMS and MMS messages, photos, videos, music, calendars, third-party app data, and purchase history from Apple, that is captured and/or stored on their personal mobile devices.

30. Based on a review of information from Apple and the examination of the iPhone 6s that was seized by the FBI on January 17, 2020, Barasneh's iCloud account appears to have backed up information that may be relevant to this investigation, including data from calendars, notes, photos, contacts, game center, iMessages, SMS and MMS, third-party apps, and browser history.

31. From my training and experience, I know that Apple customers may use the iCloud to backup their mobile devices, including iPhones, iPads and Macs, as a way to ensure that important information is not lost as well as to a means to save important information that is taking up to much space on their mobile device. It is also a way to ensure that when a mobile device is replaced – either for an upgrade or because a device has been lost, stolen or damaged, the Apple customer can restore data to the new phone. Relatedly, I understand that items that may have been accidentally or intentionally deleted or otherwise unrecoverable from a device may remain in iCloud account.

INFORMATION REGARDING APPLE ID AND iCloud³

32. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

33. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop

³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used

to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

34. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud

services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

35. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

36. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address

(“IP address”) used to register and access the account, and other log files that reflect usage of the account.

37. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

38. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play

content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

39. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

40. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

41. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

42. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or

other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

44. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. In this case, Barasneh was known to use certain apps and websites to communicate with other members of the Base and coconspirators.

45. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence

of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

46. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

49. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with barasnehyousef@gmail.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"),

Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from March 1, 2019 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from March 1, 2019 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant

message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfohist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 241 involving Yousef Omar Barasneh since March 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Records and information relating to a conspiracy to injure, oppress, threaten, and intimidate minority citizens, including Jewish citizens, in the free exercise of their legal rights, including the right to hold and use real and personal property in the same manner as that right is enjoyed by white citizens, as guaranteed by Title 42, United States Code, Section 1982;
- b. Records and information relating the organization known as The Base, associates of The Base, or white supremacy ideology, including any communications;
- c. Records and information relating to the Beth Israeli Sinai Congregation;
- d. Records and information relating to targets or potential targets of threats, harassment, or intimidation by the Base or otherwise based on white supremacist ideology
- e. The identity of the person(s) who created or used the Apple ID;

f. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

g. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

h. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple, as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature